Polar codes for the two-user multiple-access channel

Eren Şaşoğlu, Emre Telatar, Edmund Yeh

Abstract

Arıkan's polar coding method is extended to two-user multiple-access channels. It is shown that if the two users of the channel use the Arıkan construction, the resulting channels will polarize to one of five possible extremals, on each of which uncoded transmission is optimal. The sum rate achieved by this coding technique is the one that correponds to uniform input distributions. The encoding and decoding complexities and the error performance of these codes are as in the single-user case: $O(n \log n)$ for encoding and decoding, and $o(\exp(-n^{1/2-\epsilon}))$ for block error probability, where n is the block length.

I. Introduction

Polar coding, invented by Arıkan [1], is a technique for achieving the 'symmetric capacity' of binary input, memoryless channels. The underlying principle of the technique is to convert repeated uses of a given single-user channel to single uses of a set of extremal channels—almost every channel in the set is either almost perfect, or almost useless. Arıkan calls this phenomenon *polarization*. In this note we describe a way to extend this technique to multiple-access channels (MACs).

One way to do this extension is via the 'rate splitting/onion peeling' scheme of [2], [3]. In Appendix A, we describe how arbitrary points in the capacity region of a given MAC can be achieved using polar codes and rate splitting techniques.

The approach taken in here is different, partly because our motivation is to see whether multiple-access channels polarize in the same way as single-user channels do. In the following, we will describe a technique to 'polarize' a given two-user multiple-access channel in the same sense as in [1], i.e., we will convert repeated uses of this MAC into single uses of extremal MACs. Whereas in the single user case there are only two extremal channels (perfect or useless), we will see that in the multiple-access case there will be five.

The coding scheme that results from this construction shares some properties of the single-user case: the encoding and decoding complexity is $O(n \log n)$, n being the block length, and the block error probability is roughly $O(2^{-\sqrt{n}})$. Also analogous to the single-user polar codes' achieving the 'symmetric capacity', codes for the multiple-access channel are capable of achieving some of the rate pairs on the dominant face of the rate region obtained with uniformly distributed inputs.

II. Preliminaries

Let $P\colon \mathcal{X} \times \mathcal{W} \to \mathcal{Y}$ be a two user multiple-access channel with input alphabets $\mathcal{X} = \mathcal{W} = \mathbb{F}_q = \{0, 1, \dots, q-1\}$, where q is a prime number. The output alphabet $\mathcal{Y}$ may be arbitrary. The channel is specified by $P(y|x,w)$, the conditional probability of each output symbol $y \in \mathcal{Y}$ for each possible input symbol pair $(x,w) \in \mathcal{X} \times \mathcal{W}$. The capacity region of such a channel is given by

$$\mathfrak{C}(P) := \operatorname{co}\Big(\bigcup_{X,W} \mathfrak{R}(X,W)\Big)$$

where

$$\begin{aligned}\mathfrak{R}(W,X) = \big\{(R_1,R_2)\colon\ & 0 \le R_1 \le I(X;YW),\\ & 0 \le R_2 \le I(W;YX),\\ & R_1 + R_2 \le I(XW;Y)\big\},\end{aligned}$$

the union is over all random variables $X \in \mathcal{X}$, $W \in \mathcal{W}$, and $Y \in \mathcal{Y}$ jointly distributed as

$$p_{XWY}(x,w,y) = p_X(x) p_W(w) P(y \mid x,w),$$

and $\operatorname{co}(S)$ denotes the convex hull of the set S[1] .

In this note, rather than the capacity region, we will be interested in the region

$$\mathfrak{I}(P) := \mathfrak{R}(X,W) \quad \text{where } X \text{ and } W \text{ are \textit{uniformly distributed} on } \mathbb{F}_q.$$

Given such a channel P and independent random variables X, W uniformly distributed on $\mathbb{F}_q$, define

$$I^{(1)}(P) := I(X;YW), \quad I^{(2)}(P) := I(W;YX), \text{ and } I^{(12)}(P) := I(XW;Y),$$

and let

$$\mathcal{K}(P) := \big(I^{(1)}(P), I^{(2)}(P), I^{(12)}(P)\big) \in \mathbb{R}^3.$$

[1]All logarithms in this note will be to the base q. This in particular implies that $I(X;YW), I(W;YX) \in [0,1]$ and $I(XW;Y) \in [0,2]$.

Note that the region $\mathfrak{I}(P)$ is defined by

$$\mathfrak{I}(P) = \big\{(R_1, R_2)\colon 0 \le R_1 \le I^{(1)}(P),\ 0 \le R_2 \le I^{(2)}(P),\ R_1 + R_2 \le I^{(12)}(P)\big\}.$$

Further note that $\max\{I^{(1)}, I^{(2)}\} \le I^{(12)} \le I^{(1)} + I^{(2)}$, therefore the constraints that define $\mathfrak{I}(P)$ are polymatroidal. In particular, there exists $(R_1, R_2) \in \mathfrak{I}(P)$ for which $R_1 + R_2 = I^{(12)}$. The set of such points is called the *dominant face* of $\mathfrak{I}(P)$.

III. Polarization

Two independent uses of P yields a multiple-access channel P^2 with input alphabets $\mathcal{X}^2$ and $\mathcal{W}^2$, and output alphabet $\mathcal{Y}^2$. Setting the inputs (X_1, X_2, W_1, W_2) to be independent and uniformly distributed on $\mathbb{F}_q$, and letting (Y_1, Y_2) denote the output, the region $\mathfrak{I}(P^2)$ is described by the three quantities

$$\begin{aligned} &I(X_1X_2; Y_1Y_2W_1W_2) = 2I^{(1)}(P),\\ &I(W_1W_2; Y_1Y_2X_1X_2) = 2I^{(2)}(P), \quad \text{and}\\ &I(X_1X_2W_1W_2; Y_1Y_2) = 2I^{(12)}(P)\end{aligned}$$

that upper bound R_1, R_2 and $R_1 + R_2$ respectively. Now consider putting the pair $(X_1, X_2) \in \mathbb{F}_q^2$ in one-to-one correspondence with $(U_1, U_2) \in \mathbb{F}_q^2$ via

$$X_1 = U_1 + U_2, \quad X_2 = U_2$$

and the pair $(W_1, W_2) \in \mathbb{F}_q^2$ in one-to-one correspondence with $(V_1, V_2) \in \mathbb{F}_q^2$ via

$$W_1 = V_1 + V_2, \quad W_2 = V_2,$$

where both additions are modulo-q. Observe that (U_1, U_2, V_1, V_2) are also independent and uniformly distributed on $\mathbb{F}_q$. Note further that

$$\begin{aligned} 2I^{(1)}(P) &= I(X_1X_2; Y_1Y_2W_1W_2)\\ &= I(U_1U_2; Y_1Y_2V_1V_2)\\ &= I(U_1; Y_1Y_2V_1V_2) + I(U_2; Y_1Y_2V_1V_2U_1)\\ &\ge I(U_1; Y_1Y_2V_1) + I(U_2; Y_1Y_2V_1V_2U_1), \end{aligned} \tag{1}$$

$$\begin{aligned} 2I^{(2)}(P) &= I(W_1W_2; Y_1Y_2X_1X_2)\\ &= I(V_1V_2; Y_1Y_2U_1U_2)\\ &= I(V_1; Y_1Y_2U_1U_2) + I(V_2; Y_1Y_2U_1U_2V_1)\\ &\ge I(V_1; Y_1Y_2U_1) + I(V_2; Y_1Y_2U_1U_2V_1), \end{aligned} \tag{2}$$

and

$$\begin{aligned} 2I^{(12)}(P) &= I(X_1X_2W_1W_2; Y_1Y_2)\\ &= I(U_1U_2V_1V_2; Y_1Y_2)\\ &= I(U_1V_1; Y_1Y_2) + I(U_2V_2; Y_1Y_2U_1V_1). \end{aligned} \tag{3}$$

Observe that the quantities

$$I(U_1; Y_1Y_2V_1), \quad I(V_1; Y_1Y_2U_1), \quad \text{and} \quad I(U_1V_1; Y_1Y_2)$$

are those that describe the region associated to the q-ary input multiple-access channel $U_1V_1 \to Y_1Y_2$, and the quantities

$$I(U_2; Y_1Y_2V_1V_2U_1), \quad I(V_2; Y_1Y_2U_1U_2V_1), \quad \text{and} \quad I(U_2V_2; Y_1Y_2U_1V_1)$$

are those that describe the region associated to the q-ary input multiple-access channel $U_2V_2 \to Y_1Y_2U_1V_1$. This motivates the following.

Definition 4: Suppose $P\colon \mathcal{X} \times \mathcal{W} \to \mathcal{Y}$ is a two user multiple-access channel with input alphabet $\mathbb{F}_q$. Define two new multiple-access channels, $P^-\colon \mathcal{X} \times \mathcal{W} \to \mathcal{Y} \times \mathcal{Y}$ and $P^+\colon \mathcal{X} \times \mathcal{W} \to \mathcal{Y} \times \mathcal{Y} \times \mathcal{X} \times \mathcal{W}$ as:

$$P^-(y_1, y_2|u_1, v_1) = \sum_{u_2 \in \mathcal{X}} \sum_{v_2 \in \mathcal{W}} \tfrac{1}{q^2} P(y_1|u_1 + u_2, v_1 + v_2) P(y_2|u_2, v_2),$$
$$P^+(y_1, y_2, u_1, v_1|u_2, v_2) = \tfrac{1}{q^2} P(y_1|u_1 + u_2, v_1 + v_2) P(y_2|u_2, v_2).$$

The channels P^- and P^+ correspond to $U_1V_1 \to Y_1Y_2$ and $U_2V_2 \to Y_1Y_2U_1V_1$ above, respectively. It is clear that the channel P^- can be *synthesized* from two independent uses of the channel P, whereas the channel P^+ in general cannot, since

at its output we require (U_1, V_1) in addition to (Y_1, Y_2). However, P^+ can be synthesized from two uses of the channel P with the aid of a *genie* that delivers (U_1, V_1) as side information to the output terminal.

Note that the channel P^- is 'worse' and the channel P^+ is 'better' than the channel P in the sense that $I^{(\alpha)}(P^-) \leq I^{(\alpha)}(P) \leq I^{(\alpha)}(P^+)$ for each $\alpha \in \{1, 2, 12\}$. To see this, observe that if we process the output (y_1, y_2, u_1, v_1) of the channel P^+ to keep only y_2, the resulting channel is identical to P. Thus $I^{(\alpha)}(P^+) \geq I^{(\alpha)}(P)$. That $I^{(\alpha)}(P^-) \leq I^{(\alpha)}(P)$ then follows from (1), (2) and (3). Consequently,

$$\mathfrak{I}(P^-) \subset \mathfrak{I}(P) \subset \mathfrak{I}(P^+).$$

Furthermore, by virtue of equations (1), (2) and (3),

$$\tfrac{1}{2}\mathfrak{I}(P^-) + \tfrac{1}{2}\mathfrak{I}(P^+) \subset \mathfrak{I}(P),$$

where the left-hand side of the above denotes set sum, i.e.,

$$\tfrac{1}{2}\mathfrak{I}(P^-) + \tfrac{1}{2}\mathfrak{I}(P^+) = \left\{ \tfrac{1}{2}a + \tfrac{1}{2}b \colon a \in \mathfrak{I}(P^-), b \in \mathfrak{I}(P^+) \right\}.$$

Nevertheless, by the polymatroidal nature of $(I^{(1)}, I^{(2)}, I^{(12)})$ and by (3), there are points in $\frac{1}{2}\mathfrak{I}(P^-) + \frac{1}{2}\mathfrak{I}(P^+)$ that are on the dominant face of $\mathfrak{I}(P)$.

We have now seen that from two independent copies of a q-ary input multiple-access channel P we can derive two q-ary input multiple-access channels P^- and P^+. Applying the same process to P^- and P^+, we can derive from four independent copies of P, four q-ary input multiple-access channels $P^{--} := (P^-)^-$, $P^{-+} := (P^-)^+$, $P^{+-} := (P^+)^-$ and $P^{++} := (P^+)^+$. Recursively applying the process ℓ times results in 2^ℓ q-ary input multiple-access channels

$$P^{-\cdots-}, \ldots, P^{+\cdots+}.$$

These channels have the property that the set

$$2^{-\ell} \sum_{\mathbf{s}} \mathfrak{I}(P^{\mathbf{s}})$$

is a subset of $\mathfrak{I}(P)$, but contains points on the dominant face of $\mathfrak{I}(P)$.

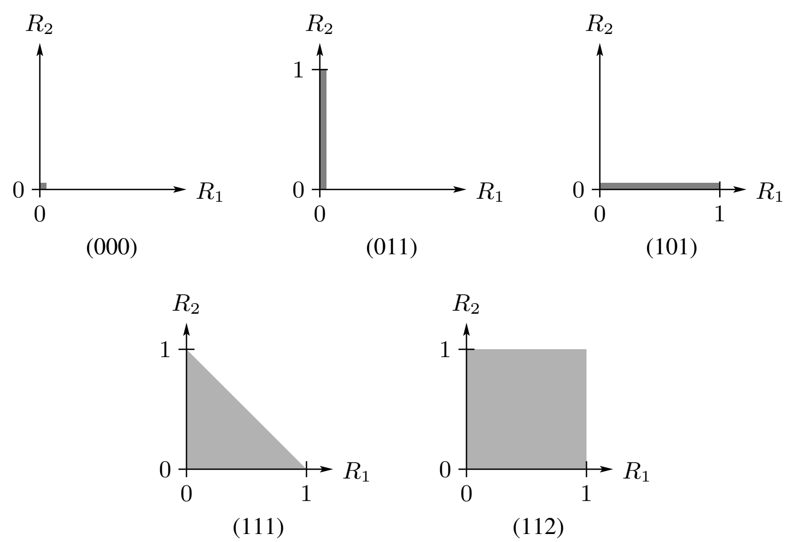
The main result reported in this section is that these derived channels polarize in the following sense:

Theorem 5: Let P be a q-ary input multiple-access channel. Let $M := \{(0,0,0), (0,1,1), (1,0,1), (1,1,1), (1,1,2)\} \subset \mathbb{R}^3$, and for $p \in \mathbb{R}^3$, let $d\big(p, M\big) := \min_{x \in M} \|p - x\|$ denote the distance from a point p to M. Then, for any $\delta > 0$

$$\lim_{\ell \to \infty} \frac{1}{2^\ell} \#\big\{\mathbf{s} \in \{-,+\}^\ell \colon d\big(\mathcal{K}(P^{\mathbf{s}}), M\big) \geq \delta\big\} = 0.$$

That is, except for a vanishing fraction, the regions $\mathfrak{I}(P^{\mathbf{s}})$ approach one of five possible regions.

Remark 6: The five limiting regions in Theorem 5 are the following.



The first case, (000), is that of a channel whose output provides no useful information about any of its inputs; the second and third, (011) and (101), are channels that provide complete information about one of the inputs but nothing about the other; the fourth, (111), is a pure contention channel; the last, (112), is one whose output determines both inputs perfectly.

Theorem 5 will be proved as a corollary to Theorem 13 below. To prove the latter theorem, we need a few auxiliary results:

Lemma 7 ([6]): For any $\epsilon > 0$, there is a $\delta := \delta(\epsilon) > 0$ such that if

(i) $Q \colon \mathbb{F}_q \to \mathcal{B}$ is a q-ary input channel with arbitrary output alphabet $\mathcal{B}$, and

(ii) A_1, A_2, B_1, B_2 are random variables jointly distributed as

$$p_{A_1A_2B_1B_2}(a_1, a_2, b_1, b_2) = \tfrac{1}{q^2} Q(b_1|a_1 + a_2) Q(b_2|a_2), \quad \text{and}$$

(iii) $I(A_2; B_1B_2A_1) - I(A_2; B_2) < \delta$,

then,

$$I(A_2; B_2) \notin (\epsilon, 1 - \epsilon).$$

Note that δ can be chosen irrespective of the alphabet $\mathcal{B}$.

Corollary 8: For any $\epsilon > 0$ there exists a $\delta > 0$ such that if P is a two-user q-ary input multiple-access channel with

$$I^{(1)}(P^+) - I^{(1)}(P) < \delta,$$

then, $I^{(1)}(P) \notin (\epsilon, 1 - \epsilon)$. Similarly, if P is such that

$$I^{(2)}(P^+) - I^{(2)}(P) < \delta,$$

then, $I^{(2)}(P) \notin (\epsilon, 1 - \epsilon)$.

Proof: It suffices to prove the first claim. To that end, note that $I^{(1)}(P) = I(U_2; Y_2V_2)$ and $I^{(1)}(P^+) = I(U_2; Y_1Y_2U_1V_1V_2)$, where

$$p_{U_1V_1U_2V_2Y_1Y_2}(u_1, v_1, u_2, v_2, y_1, y_2) = \tfrac{1}{q^4} P(y_1 \mid u_1 + u_2, v_1 + v_2) P(y_2 \mid u_2, v_2).$$

We have by hypothesis that

$$\delta > I(U_2; Y_1Y_2V_1V_2U_1) - I(U_2; Y_2V_2).$$

It can easily be checked that the values of the above mutual informations remain unaltered if evaluated under the joint distribution

$$q_{U_1V_1U_2V_2Y_1Y_2}(u_1, v_1, u_2, v_2, y_1, y_2) = \tfrac{1}{q^4} P(y_1 \mid u_1 + u_2, v_1) P(y_2 \mid u_2, v_2).$$

Defining $A_i = U_i$, $B_i = (Y_i, V_i)$ and $Q(y, v|u) = \frac{1}{2} P(y|u, v)$, one can then write

$$q_{A_1A_2B_1B_2}(a_1, a_2, b_1, b_2) = \tfrac{1}{q^2} Q(b_1 \mid a_1 + a_2) Q(b_2 \mid a_2).$$

Applying Lemma 7 now yields the claim. ■

Lemma 9: For any $\epsilon > 0$ there exists a $\delta > 0$ such that whenever P is a two-user q-ary input multiple-access channel with $I^{(12)}(P^+) - I^{(12)}(P) < \delta$, then

$$I^{(12)}(P) - I^{(j)}(P) \notin (\epsilon, 1 - \epsilon) \quad \text{for } j = 1, 2.$$

Proof: By symmetry, it suffices to prove the claim for $j = 1$. Choose δ so that $\delta < \epsilon$ and $\delta < \delta(\epsilon)$ of Lemma 7. Note that

$$\begin{aligned}
\delta &> I^{(12)}(P^+) - I^{(12)}(P) \\
&= I(U_2V_2; Y_1Y_2U_1V_1) - I(U_2V_2; Y_2) \\
&= I(U_2V_2; Y_1U_1V_1|Y_2) \\
&\geq I(U_2; Y_1U_1|Y_2) \\
&= I(U_2; Y_1Y_2U_1) - I(U_2; Y_2).
\end{aligned}$$

Applying Lemma 7 with $A_i = U_i$, $B_i = Y_i$ and $Q(y|u) = \sum_v \frac{1}{q} P(y|u, v)$ we conclude that $I(U_2; Y_2) \notin (\epsilon, 1 - \epsilon)$. Since $I(U_2; Y_2) = I^{(12)}(P) - I^{(1)}(P)$, the claim follows. ■

Suppose P is a two-user q-ary input MAC. Let $B_1, B_2, \ldots$ be an i.i.d. sequence of random variables taking values in the set $\{-, +\}$, with $\Pr(B_1 = -) = \Pr(B_1 = +) = 1/2$. Define a *MAC-valued* random process $\{P_\ell : \ell \geq 0\}$ via

$$P_0 := P, \quad P_\ell := P_{\ell-1}^{B_\ell}, \; \ell \geq 1. \tag{10}$$

Further define random processes $\{I_\ell^{(1)} : \ell \geq 0\}$, $\{I_\ell^{(2)} : \ell \geq 0\}$ and $\{I_\ell^{(12)} : \ell \geq 0\}$ as

$$I_\ell^{(1)} := I^{(1)}(P_\ell), \quad I_\ell^{(2)} := I^{(2)}(P_\ell), \quad \text{and} \quad I_\ell^{(12)} := I^{(12)}(P_\ell). \tag{11}$$

Lemma 12: The processes $\{I_\ell^{(1)} : \ell \geq 0\}$ and $\{I_\ell^{(2)} : \ell \geq 0\}$ are bounded supermartingales, the process $\{I_\ell^{(12)} : \ell \geq 0\}$ is a bounded martingale.

Proof: Since P_ℓ is a q-ary input MAC, $I_\ell^{(1)}$ and $I_\ell^{(2)}$ take values is $[0, 1]$ and $I_\ell^{(12)}$ takes values in $[0, 2]$, and thus the processes are bounded. The martingale claims follow from (1), (2) and (3) respectively. ■

Theorem 13: The process $(I_\ell^{(1)}, I_\ell^{(2)}, I_\ell^{(12)})$ converges almost surely, and the limit

$$(I_\infty^{(1)}, I_\infty^{(2)}, I_\infty^{(12)}) := \lim_{\ell \to \infty} (I_\ell^{(1)}, I_\ell^{(2)}, I_\ell^{(12)})$$

belongs to the set $\{(0,0,0),(0,1,1),(1,0,1),(1,1,1),(1,1,2)\}$ with probability 1.

Proof: Let $(\Omega, \Pr, \mathcal{F})$ be the probability space these processes are defined in. Let

$$A := \big\{\omega \in \Omega \colon \lim_{\ell\to\infty} I_\ell^{(\alpha)} \text{ exists for each } \alpha \in \{1,2,12\}\big\}.$$

The almost sure convergence of $I_\ell^{(1)}$ and $I_\ell^{(2)}$ follow from them being bounded supermartingales, almost sure convergence of $I_\ell^{(12)}$ follows form it being a bounded martingale. Thus, $\Pr(A)=1$, and it remains to show that the joint limit belongs to the set claimed.

To that end we will first show that $I_\infty^{(1)} \in \{0,1\}$ a.s. Since $I_\ell^{(1)}$ converges a.s., $\lim_{\ell\to\infty}|I_{\ell+1}^{(1)} - I_\ell^{(1)}| = 0$ a.s. Since $|I_{\ell+1}^{(1)} - I_\ell^{(1)}|$ is bounded (by 1), it follows that $\lim_{\ell\to\infty} E\big[|I_{\ell+1}^{(1)} - I_\ell^{(1)}|\big] = 0$. But

$$E\big[|I_{\ell+1}^{(1)} - I_\ell^{(1)}|\big] \ge \tfrac{1}{2}\big[I^{(1)}(P_\ell^+) - I^{(1)}(P_\ell)\big],$$

and we see that $\lim_{\ell\to\infty} I^{(1)}(P_\ell^+) - I^{(1)}(P_\ell) = 0$. From Corollary 8 we conclude that $\lim_{\ell\to\infty} I_\ell^{(1)} \in \{0,1\}$.

Swapping the roles of the two users yields $I_\infty^{(2)} \in \{0,1\}$ a.s. We thus find that $(I_\infty^{(1)}, I_\infty^{(2)})$ is equal to either $(0,0)$, $(0,1)$, $(1,0)$, or $(1,1)$. Denoting the set of $\omega \in A$ for which $I_\infty^{(1)} = a$, $I_\infty^{(2)} = b$ by A_{ab}, we see that $A = A_{00} \cup A_{01} \cup A_{10} \cup A_{11}$. Since

$$\max\{I^{(1)}, I^{(2)}\} \le I^{(12)} \le I^{(1)} + I^{(2)},$$

we conclude that the value of $I_\infty^{(12)}$ in A_{00}, A_{01} and A_{10} is 0, 1, and 1 respectively.

All that remains now is to show that $I_\infty^{(12)}$ belongs to $\{1,2\}$ for $\omega \in A_{11}$. To that end note that for any $\omega \in A_{11}$,

(i) $\lim_{\ell\to\infty} I^{(1)}(P_\ell) = 1$, $\lim_{\ell\to\infty} I^{(2)}(P_\ell) = 1$, and

(ii) $\lim_{\ell\to\infty} I^{(12)}(P_\ell)$ exists and thus $\lim_{\ell\to\infty}\big|I^{(12)}(P_{\ell+1}) - I^{(12)}(P_\ell)\big| = 0$.

But

$$\big|I^{(12)}(P_{\ell+1}) - I^{(12)}(P_\ell)\big| = I^{(12)}(P_\ell^+) - I^{(12)}(P_\ell),$$

and thus $\lim_{\ell\to\infty} I^{(12)}(P_\ell^+) - I^{(12)}(P_\ell) = 0$. Now Lemma 9 lets us conclude that $\lim_{\ell\to\infty} I^{(12)}(P_\ell) \in \{1,2\}$. ■

Proof of Theorem 5: When the processes P_ℓ and $(I_\ell^{(1)}, I_\ell^{(2)}, I_\ell^{(12)})$, $\ell = 0,1,\dots$ are defined as in (10) and (11), respectively, we have

$$\Pr\big[d((I_\ell^{(1)}, I_\ell^{(2)}, I_\ell^{(12)}), M) \ge \delta\big] = \frac{1}{2^\ell}\#\big\{\mathbf{s} \in \{-,+\}^\ell \colon d(\mathcal{K}(P^{\mathbf{s}}), M) \ge \delta\big\}.$$

The claim then follows from Theorem 13.

IV. Rate of Polarization

We have seen that any q-ary input MAC can be polarized to a set of five extremal MACs, by recursively applying the channel combining/splitting procedure of Section III. Furthermore, Remark 6 suggests a natural scheme to exploit this phenomenon—polar coding [1]: one can hope to communicate reliably by sending uncoded information over the reliable channels, and not sending any information over the others. In this section, we will formalize this intuition, showing that such a coding scheme achieves points on the dominant face of $\mathfrak{I}(P)$.

We first introduce some notation: Given a q-ary input multiple-access channel P, define two point-to-point channels $P[U] \colon \mathbb{F}_q \to \mathcal{Y}$ and $P[U \mid V] \colon \mathbb{F}_q \to \mathcal{Y} \times \mathbb{F}_q$ through

$$P[U](y \mid u) = \tfrac{1}{q}\sum_v P(y \mid u, v)$$

$$P[U \mid V](y, v \mid u) = \tfrac{1}{q}P(y \mid u, v)$$

That is, $P[U]$ is the channel $U \to Y$, and $P[U \mid V]$ is the channel $U \to YV$. Define $P[V]$ and $P[V \mid U]$ analogously. Also, for every $\alpha, \gamma \in \mathbb{F}_q$ define the channels $P[\alpha,\gamma] \colon \mathbb{F}_q \to \mathcal{Y}$ through

$$P[\alpha,\gamma](y \mid s) = \tfrac{1}{q}\sum_{\substack{u,v\colon\\ \alpha u + \gamma v = s}} P(y \mid u, v)$$

That is, $P[\alpha,\gamma]$ is the channel $\alpha U + \gamma V \to Y$.

Given a point-to-point channel $Q \colon \mathbb{F}_q \to \mathcal{Y}$, let $P_e(Q)$ denote its average probability of error with uniform input distribution and the optimal (ML) decision rule. Also let $I(Q)$ denote the mutual information developed across Q with uniform inputs. That is,

$$I(Q) = \tfrac{1}{q}\sum_{x,y} Q(y \mid x)\log\frac{Q(y \mid x)}{\tfrac{1}{q}\sum_{x'} Q(y \mid x')}.$$

Finally let $Z(Q)$ define the *Bhattacharyya parameter* of Q, defined as

$$Z(Q) = \tfrac{1}{q(q-1)} \sum_{x \neq x'} \sum_{y \in \mathcal{B}} \sqrt{Q(y \mid x) Q(y \mid x')}.$$

It is known (see [5]) that $P_e(Q) \leq qZ(Q)$.

We are now ready to describe the encoding rule: Fix ℓ and let $n = 2^\ell$. Let B_n denote the $n \times n$ permutation matrix called the 'bit reversal' operator in [1], and let $G_n = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]^{\otimes \ell}$ denote the ℓth Kronecker power of the matrix $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$. Put $U^n := (U_1, \dots, U_n)$ and $V^n = (V_1, \dots, V_n)$ into one-to-one correspondence with $X^n = (X_1, \dots, X_n)$ and $W^n = (W_1, \dots, W_n)$ via

$$X^n = U^n B_n G_n,$$
$$W^n = V^n B_n G_n.$$

Transmit (X^n, W^n) over n independent uses of P and receive Y^n. Defining $P_{(i)} \colon \mathcal{X} \times \mathcal{W} \to \mathcal{Y}^n \times \mathcal{X}^{i-1} \times \mathcal{W}^{i-1}$ to be the channel $U_i V_i \to Y^n U^{i-1} V^{i-1}$, we see that

$$\begin{aligned} P_{(1)} &\text{ is } P^{-\cdots--}; \\ P_{(2)} &\text{ is } P^{-\cdots-+}; \\ P_{(3)} &\text{ is } P^{-\cdots+-}; \\ &\vdots \\ P_{(n)} &\text{ is } P^{+\cdots++}. \end{aligned}$$

It then follows from Theorem 5 that when n is large, almost all channels $P_{(i)}$ are close to one of the five limiting channels. Also note that the ith channel assumes a genie that provides knowledge of the previous symbols $(U^{i-1} V^{i-1})$ at the receiver. This observation and Remark 6 motivate the following coding scheme: Fix $\epsilon > 0$, $\delta > 0$. Let $\mathcal{A}_U \subset (U_1, \dots, U_n)$ and $\mathcal{A}_V \subset (V_1, \dots, V_n)$ denote the sets of information symbols to be transmitted. Choose these sets as follows:

(i) If $\|\mathcal{K}(P_{(i)}) - (0,0,0)\| < \epsilon$ then $U_i \notin \mathcal{A}_U, V_i \notin \mathcal{A}_V$,
(s.i) if $\|\mathcal{K}(P_{(i)}) - (0,1,1)\| < \epsilon$ then $U_i \notin \mathcal{A}_U, V_i \in \mathcal{A}_V$,
(s.ii) if $\|\mathcal{K}(P_{(i)}) - (1,0,1)\| < \epsilon$ then $U_i \in \mathcal{A}_U, V_i \notin \mathcal{A}_V$,
(s.iii) if $\|\mathcal{K}(P_{(i)}) - (1,1,1)\| < \epsilon$ then either $U_i \in \mathcal{A}_U, V_i \notin \mathcal{A}_V$, or $U_i \notin \mathcal{A}_U, V_i \in \mathcal{A}_V$,
(s.iv) if $\|\mathcal{K}(P_{(i)}) - (1,1,2)\| < \epsilon$ then $U_i \in \mathcal{A}_U, V_i \in \mathcal{A}_V$,
(s.v) otherwise, $U_i \notin \mathcal{A}_U, V_i \notin \mathcal{A}_V$.

Choose the symbols in $\mathcal{A}_U^c$ and $\mathcal{A}_V^c$ independently and uniformly at random, and reveal their values to the receiver. This choice of $\mathcal{A}_U$ and $\mathcal{A}_V$ ensures that all the information symbols see 'reliable' channels, provided that the previous symbols are decoded correctly. Consequently, upon receiving Y^n, the receiver may attempt to decode the symbols successively, in the order $(U_1 V_1)$, $(U_2 V_2) \dots$, and hope for a low block error probability. Furthermore, Theorem 5 and the preservation of $I^{(12)}(P)$ throughout the recursive channel splitting/combining process guarantee that for any choice of ϵ and δ there exists n_0 such that $|\mathcal{A}_U| + |\mathcal{A}_V| > n[I^{(12)}(P) - \delta]$ whenever $n \geq n_0$. This observation hints at the achievability of points on the dominant face of $\mathfrak{I}(P)$. For a proof of achievability, it only remains to show that the block error probability of the discussed scheme vanishes with increasing block length. We do this next.

Let $\phi_i \colon \mathcal{Y}^n \times \mathbb{F}_q^{i-1} \times \mathbb{F}_q^{i-1}$, $i = 1, \dots, n$ denote the ML decision rule for estimating $(U_i V_i)$ given $(Y^n, (UV)^{i-1})$. Note that this corresponds to a *genie aided* decision rule—the genie provides $(UV)^{i-1}$—for estimating $(U_i V_i)$ from the output Y^n. Let E_i denote the event $\phi_i(Y^n, (UV)^{i-1}) \neq (U_i V_i)$. Observe that E_i is precisely the error event of $P_{(i)}$. Now define a standalone decoder, recursively through

$$T_i = \phi_i(Y^n, T^{i-1}), \qquad i = 1, \dots, n,$$

and let E'_i denote the event $T_i \neq (U_i V_i)$. Note that $\cup_i E'_i$ is the block error event for the scheme discussed above, and that

$$\cup_i E_i = \cup_i E'_i.$$

Hence, the block error probability can be bounded as

$$\Pr[\text{block error}] = \Pr[\cup_i E'_i] = \Pr[\cup_i E_i] \leq \sum_i \Pr[E_i] = \sum_i P_e(P_{(i)}). \tag{14}$$

Note that the transmission scheme described above implies that the only non-zero error terms on the right-hand-side of (14) are those corresponding to the symbols in $\mathcal{A}_U$ and $\mathcal{A}_V$. We will show that almost all of these terms are sufficiently small, i.e., that by removing a negligible fraction of information bits from $\mathcal{A}_U$ and $\mathcal{A}_V$, the above sum can be made to vanish.

Theorem 15: For any $\beta < 1/2$, the block error probability of the polar coding scheme described above, under successive cancellation decoding, is $o(2^{-n^\beta})$.

Theorem 15 is an immediate corollary to the following result.

Lemma 16: For any $\epsilon > 0$ and $\beta < 1/2$,

(r.1) $\lim_{\ell\to\infty} \frac{1}{2^\ell} \# \left\{ \mathbf{s} \in \{-,+\}^\ell : \|\mathcal{K}(P^{\mathbf{s}}) - (0,1,1)\| < \epsilon, P_e(P^{\mathbf{s}}[V]) \geq 2^{-2^{\ell\beta}} \right\} = 0,$

(r.2) $\lim_{\ell\to\infty} \frac{1}{2^\ell} \# \left\{ \mathbf{s} \in \{-,+\}^\ell : \|\mathcal{K}(P^{\mathbf{s}}) - (1,0,1)\| < \epsilon, P_e(P^{\mathbf{s}}[U]) \geq 2^{-2^{\ell\beta}} \right\} = 0,$

(r.3) $\lim_{\ell\to\infty} \frac{1}{2^\ell} \# \left\{ \mathbf{s} \in \{-,+\}^\ell : \|\mathcal{K}(P^{\mathbf{s}}) - (1,1,1)\| < \epsilon, \max\{P_e(P^{\mathbf{s}}[U \mid V]), P_e(P^{\mathbf{s}}[V \mid U])\} \geq 2^{-2^{\ell\beta}} \right\} = 0,$

(r.4) $\lim_{\ell\to\infty} \frac{1}{2^\ell} \# \left\{ \mathbf{s} \in \{-,+\}^\ell : \|\mathcal{K}(P^{\mathbf{s}}) - (1,1,2)\| < \epsilon, P_e(P^{\mathbf{s}}[U]) + P_e(P^{\mathbf{s}}[V]) \geq 2^{-2^{\ell\beta}} \right\} = 0.$

The following proposition will be useful in the proof of Lemma 16.

Proposition 17: For all $\alpha, \gamma \in \mathbb{F}_q$ and $\delta > 0$,

$$\lim_{\ell\to\infty} \frac{1}{2^\ell} \# \left\{ \mathbf{s} \in \{-,+\}^\ell : I(P^{\mathbf{s}}[\alpha,\gamma]) \in (\delta, 1-\delta) \right\} = 0. \tag{18}$$

That is, the channels $\alpha U + \gamma V \to Y$ polarize to become either perfect or useless. Moreover, convergence to perfect channels is almost surely fast:

$$\lim_{\ell\to\infty} \frac{1}{2^\ell} \# \left\{ \mathbf{s} \in \{-,+\}^\ell : I(P^{\mathbf{s}}[\alpha,\gamma]) \geq 1-\delta, Z(P^{\mathbf{s}}[\alpha,\gamma]) \geq 2^{-n^\beta} \right\} = 0 \tag{19}$$

for all $0 < \beta, \delta < 1/2$ and $\alpha, \gamma \in \mathbb{F}_q$.

Proof: See Appendix B. ∎

Proof of Lemma 16: The proof of (r.1) follows immediately from Proposition 17 by taking $\alpha = 0$ and $\gamma = 1$, and by the relation $P_e(P^{\mathbf{s}}[V]) \leq qZ(P^{\mathbf{s}}[V])$. Proofs of (r.2) and (r.4) follow similarly.

To prove (r.3), we first observe that for any MAC P,

$$\max\{P_e(P[U \mid V]), P_e(P[V \mid U])\} \leq P_e(P[\alpha,\gamma]) \leq qZ(P[\alpha,\gamma]) \tag{20}$$

for all $\alpha, \gamma \in \mathbb{F}_q$. We also know from Proposition 17 that when ℓ is sufficiently large, then for all $\alpha, \gamma \in \mathbb{F}_q$,

$$I(P^{\mathbf{s}}[\alpha,\gamma]) \notin (o(\epsilon), 1-o(\epsilon)) \tag{21}$$

for almost all $\mathbf{s} \in \{-,+\}^\ell$. It is an immediate consequence of Lemma 33 in Appendix C that whenever (21) is satisfied, then

$$\|\mathcal{K}(P^{\mathbf{s}}) - (1,1,1)\| < \epsilon \text{ implies } I(P[\alpha,\gamma]) > 1 - o(\epsilon)$$

for some α, γ. Claim (r.3) will then follow from (19) and (20).

V. Discussion

The technique described above adapts the single-user polarization technique of Arıkan to the two-user multiple-access channels. It can be seen that it retains the quality of being low complexity, and has similar error probability scaling as the single-user case.

As in the original polar code construction for single user channels, the discussion for MAC polar codes above consider uniform input distributions. How to achieve true channel capacity with polar codes, using Gallager's method [8, p. 208], is discussed in [5]. The arguments in [5, Section III.D] can easily be adapted to multiple-access channels to extend the above results to rate regions with non-uniform inputs.

A number of questions for further study come to mind: Unlike the single-user setting, where the 'symmetric capacity' of a channel is a single number, the 'dominant face' of the set of rates that correspond to uniformly distributed inputs is a line segment. The polarization technique outlined here does not in general achieve the whole segment, but only a subset of it, for the simple reason that the equations (1) and (2) are inequalities rather than equalities. Is there an alternative way to do MAC polarizaton and not suffer this loss?

A natural extension of the results presented is to the case of multiple-access channels with more than two users. For such channels, one can fairly easily show that with a similar construction as in this paper, there are a finite number of limiting MACs, and that these extremal MACs have the property that their rate regions are described by polymatroidal equations with *integer* right-hand sides, and are thus matroids. One encounters, however, a new phenomenon: not all matroids are possible regions of a MAC. The treatment of these require further techniques, which is the subject of [7].

Appendix A

In this section, we discuss how polar codes can be used to achieve arbitrary points in the capacity region of any MAC with arbitrary number of users and discrete input alphabets. We follow the notation used in Section II. For sake of simplicity, we show the achievability of corner points of $\mathfrak{I}(P)$ for a given q-ary input two-user MAC P, and discuss how the result can be generalized.

Theorem 22: Let P be a two-user q-ary input MAC. For any $\epsilon > 0$ and $\beta < 1/2$, there exist two polar codes $\mathcal{C}_1$ and $\mathcal{C}_2$ with sufficiently large block lengths n, and with rates

$$R_1 > I(X;Y) - \epsilon$$
$$R_2 > I(W;YX) - \epsilon$$

such that if used by the two senders for transmission over P, their average block error probability does not exceed 2^{-n^β}. This performance is guaranteed under a receiver that decodes the *messages* successively.

Proof: Given a single-user q-ary input channel Q, let $P_{e,n}(Q, \mathcal{A}, u_{\mathcal{A}^c})$ denote the block error probability of a polar code under successive cancellation (SC) decoding, with information set $\mathcal{A}$ and frozen symbols fixed to $u_{\mathcal{A}^c}$, averaged over all messages. We know from [1] and [5] that when n is sufficiently large, there exists a set $\mathcal{A}$ with $|\mathcal{A}| > n(I(Q) - \epsilon)$ and

$$\frac{1}{2^{|\mathcal{A}^c|}} \sum_{u_{\mathcal{A}^c}} P_{e,n}(Q, \mathcal{A}, u_{\mathcal{A}^c}) = \mathcal{O}(2^{-n^\beta}). \tag{23}$$

Define two q-ary input channels $Q_1 \colon \mathbb{F}_2 \to \mathcal{Y}$ and $Q_2 \colon \mathbb{F}_2 \to \mathcal{Y}$ through the transition probabilities

$$Q_1(y \mid x) = \tfrac{1}{q} \sum_w P(y \mid x, w),$$
$$Q_2(y, x \mid w) = \tfrac{1}{q} P(y \mid x, w).$$

Clearly, we have $I(Q_1) = I(X;Y)$ and $I(Q_2) = I(W;YX)$. Take n sufficiently large and find sets $\mathcal{A}_1$ and $\mathcal{A}_2$ with $|\mathcal{A}_1| > n(I(Q_1) - \epsilon)$ and $|\mathcal{A}_2| > n(I(Q_2) - \epsilon)$, such that (23) holds when $(Q, \mathcal{A})$ is replaced with $(Q_1, \mathcal{A}_1)$ and $(Q_2, \mathcal{A}_2)$, respectively. We will show that the ensemble of polar code pairs characterized by $\mathcal{A}_1$ and $\mathcal{A}_2$ have small average error probability when used for transmission over P.

Consider a receiver that first makes an SC estimate $\hat{X}^n = \phi_X(Y^n)$ on the first sender's codeword X^n based on the output Y^n, and then produces $\hat{W}^n = \phi_W(Y^n \hat{X}^n)$, where ϕ_W denotes the SC estimate of W^n conditioned on $(Y^n X^n)$. That is, the decoder for W^n assumes that the decision on X^n is always correct. The average block error probability of this scheme can be bounded using the relations

$$\begin{aligned}
\Pr[\text{block error}] &= \Pr[\hat{X}^n \neq X^n \text{ or } \hat{W}^n \neq W^n] \\
&= \Pr[\phi_X(Y) \neq X^n] + \Pr[\phi_W(Y^n \hat{X}^n) \neq W^n, \hat{X}^n = X^n] \\
&= \Pr[\phi_X(Y) \neq X^n] + \Pr[\phi_W(Y^n X^n) \neq W^n, \hat{X}^n = X^n] \\
&\leq \Pr[\phi_X(Y) \neq X^n] + \Pr[\phi_W(Y^n X^n) \neq W^n].
\end{aligned}$$

The first probability term above can be written as

$$\begin{aligned}
\Pr[\phi_X(Y^n) \neq X^n] &= \frac{1}{q^n} \sum_{w^n} \Pr[\phi_X(Y^n) \neq X^n \mid W^n = w^n] \\
&= \frac{1}{q^{|\mathcal{A}_1^c|}} \sum_{u_{\mathcal{A}_1^c}} P_{e,n}(Q_1, \mathcal{A}_1, u_{\mathcal{A}_1^c}) \\
&= \mathcal{O}(2^{-n^\beta}).
\end{aligned}$$

Here, we obtained the second equality by observing that the codeword symbols X^n and W^n are independent and uniformly distributed, which follows from the uniform distribution on the frozen and information symbols. The third inequality follows from (23). By the same line of argument one can write

$$\begin{aligned}
\Pr[\phi_W(Y^n X^n) \neq W^n] &= \sum_{x_1^n} \Pr[\phi_W(Y^n X^n) \neq W_1^n, X_1^n = x_1^n] \\
&= \frac{1}{q^{|\mathcal{A}_2^c|}} \sum_{u_{\mathcal{A}_2^c}} P_{e,n}(Q_2, \mathcal{A}_2, u_{\mathcal{A}_2^c}) \\
&= \mathcal{O}(2^{-n^\beta}).
\end{aligned}$$

Therefore, the block error probability, averaged over the ensemble of polar code pairs is $\mathcal{O}(2^{-n^\beta})$. This lets us conclude that there exists at least one pair of polar codes with the promised rates and average block error probability. ■

In [2] and [3], it was shown that any point in the capacity region of an M-user MAC can be expressed as a corner point of (at most) a $(2M-1)$-user MAC rate region, possibly with non-uniform inputs. In addition, it is shown in [5, Section III] how polar codes for non-binary channels can be used to achieve capacity of arbitrary discrete channels, by inducing arbitrary non-uniform distributions on the input. Modifying the above proof along these observations, one can easily generalize Theorem 22 in order to show that polar codes achieve all points in the capacity region of any discrete input MAC with arbitrary number of users.

Appendix B: Proof of Proposition 17

Given a channel $Q\colon \mathbb{F}_q \to \mathcal{Y}$, define two channels $Q^b\colon \mathbb{F}_q \to \mathcal{Y}^2$ and $Q^g\colon \mathbb{F}_q \to \mathcal{Y}^2 \times \mathbb{F}_q$ through

$$Q^b(y_1, y_2 \mid x_1) = \sum_{x_2} \tfrac{1}{2} Q(y_1 \mid x_1 + x_2) Q(y_2 \mid x_2),$$
$$Q^g(y_1, y_2, x_1 \mid x_2) = \tfrac{1}{2} Q(y_1 \mid x_1 + x_2) Q(y_2 \mid x_2).$$

It is easy to see that $I(Q^b) + I(Q^g) = 2I(Q)$. We will show that for all $\alpha, \gamma \in \mathbb{F}_q$,

(i) $P[\alpha,\gamma]^g$ is degraded with respect to $P^+[\alpha,\gamma]$,
(ii) $P[\alpha,\gamma]^b$ is equivalent to $P^+[\alpha,\gamma]$,

implying

$$I(P^+[\alpha,\gamma]) + I(P^-[\alpha,\gamma]) \geq 2I(P[\alpha,\gamma]).$$

This, in addition to (i), (ii), and Lemma 7, implies the convergence of the channels $P[\alpha,\gamma]$ to extremals—the proof is identical to that of Corollary 8. That is,

$$\lim_{\ell\to\infty} \frac{1}{2^\ell} \# \left\{ \mathbf{s} \in \{-,+\}^\ell \colon I(P^{\mathbf{s}}[\alpha,\gamma]) \in (\delta, 1-\delta) \right\} = 0.$$

To prove the claim on the rate of convergence, we will show that

$$Z(P^-[\alpha,\gamma]) \leq 2Z(P[\alpha,\gamma]) \quad \text{and} \quad Z(P^+[\alpha,\gamma]) \leq qZ(P[\alpha,\gamma])^2. \tag{24}$$

The proof will then follow from previous results, namely

Lemma 25 ([4],[5]): For any q-ary input channel $Q\colon \mathbb{F}_2 \to \mathcal{Y}$, channels Q^b and Q^g satisfy

$$Z(Q^b) \leq 2Z(Q) \quad \text{and} \quad Z(Q^g) \leq qZ(Q)^2. \tag{26}$$

In particular, this implies that

$$\lim_{\ell\to\infty} \frac{1}{2^\ell} \# \left\{ \mathbf{s} \in \{g,b\}^\ell \colon I(Q^{\mathbf{s}}) > 1-\epsilon, Z(Q^{\mathbf{s}}) > 2^{-2^{\ell\beta}} \right\} = 0 \tag{27}$$

for all $0 < \epsilon, \beta < 1/2$.
It thus remains to show (i), (ii), and (24).

Proof of (i): We have by definition

$$\begin{aligned} P^+[\alpha,\gamma](y_1, y_2, u_1, v_1 \mid s) &= \sum_{\substack{u_2, v_2: \\ \alpha u_2 + \gamma v_2 = s}} \frac{1}{q} P^+(y_1, y_2, u_1, v_1 \mid u_2, v_2) \\ &= \sum_{\substack{u_2, v_2: \\ \alpha u_2 + \gamma v_2 = s}} \tfrac{1}{q^3} P(y_1 \mid u_1 + u_2, v_1 + v_2) P(y_2 \mid u_2, v_2). \end{aligned} \tag{28}$$

On the other hand,

$$\begin{aligned} P[\alpha,\gamma]^g(y_1, y_2, x \mid s) &= \tfrac{1}{q} P[\alpha,\gamma](y_1 \mid x + s) P[\alpha,\gamma](y_2 \mid s) \\ &= \tfrac{1}{q^3} \sum_{\substack{u_1, v_1, u_2, v_2: \\ \alpha u_1 + \gamma v_1 = x + s \\ \alpha u_2 + \gamma v_2 = s}} P(y_1 \mid u_1, v_1) P(y_2 \mid u_2, v_2) \end{aligned}$$

Since the constraints $\alpha u_1 + \gamma v_1 = x + s$ and $\alpha u_2 + \gamma v_2 = s$ are linear, the above sum can be rewritten as

$$P[\alpha,\gamma]^g(y_1, y_2, u_1, v_1 \mid s) = \tfrac{1}{q^3} \sum_{\substack{u_1, v_1, u_2, v_2: \\ \alpha u_1 + \gamma v_1 = x \\ \alpha u_2 + \gamma v_2 = s}} P(y_1 \mid u_1 + u_2, v_1 + v_2) P(y_2 \mid u_2, v_2). \tag{29}$$

Comparing (28) and (29), we observe that the channel $P[\alpha,\gamma]^g$ is obtained by processing the output (Y_1, Y_2, U_1, V_1) of $P^+[\alpha,\gamma]$ to retain $(Y_1, Y_2, \alpha U_1 + \gamma V_1)$. This completes the proof.

Proof of (ii): We have

$$\begin{aligned} P^-[\alpha,\gamma](y_1, y_2, \mid x) &= \sum_{\substack{u_1, v_1: \\ \alpha u_1 + \gamma v_1 = x}} \frac{1}{q} P^-(y_1, y_2 \mid u_1, v_1) \\ &= \sum_{\substack{u_1, v_1, u_2, v_2: \\ \alpha u_1 + \gamma v_1 = x}} \tfrac{1}{q^3} P(y_1 \mid u_1 + u_2, v_1 + v_2) P(y_2 \mid u_2, v_2). \end{aligned} \tag{30}$$

On the other hand,

$$\begin{aligned} P[\alpha,\gamma]^b(y_1,y_2 \mid x) &= \tfrac{1}{q}\sum_s P[\alpha,\gamma](y_1 \mid x+s)P[\alpha,\gamma](y_2 \mid s) \\ &= \sum_{\substack{u_1,v_1,u_2,v_2:\\ \alpha u_1+\gamma v_1=x+s\\ \alpha u_2+\gamma v_2=s}} \sum_s \tfrac{1}{q^3} P(y_1 \mid u_1,v_1)P(y_2 \mid u_2,v_2) \end{aligned}$$

As in the proof of (i), we can rewrite the above sum as

$$\begin{aligned} P[\alpha,\gamma]^b(y_1,y_2,u_1,v_1 \mid s) &= \sum_{\substack{u_1,v_1,u_2,v_2:\\ \alpha u_1+\gamma v_1=x\\ \alpha u_2+\gamma v_2=s}} \sum_s \tfrac{1}{q^3} P(y_1 \mid u_1+u_2, v_1+v_2)P(y_2 \mid u_2,v_2) \\ &= \sum_{\substack{u_1,v_1,u_2,v_2:\\ \alpha u_1+\gamma v_1=x}} \tfrac{1}{q^3} P(y_1 \mid u_1+u_2, v_1+v_2)P(y_2 \mid u_2,v_2). \end{aligned} \tag{31}$$

Comparing (30) and (31) we conclude that $P[\alpha,\gamma]^b$ and $P^-[\alpha,\gamma]$ are equivalent.

Proof of (24)*:* It immediately follows from (26) and (ii) that $Z(P^b[\alpha,\gamma]) \leq 2Z(P[\alpha,\gamma])$. In order to complete the proof, we will show that $Z(P^+[\alpha,\gamma]) \leq Z(P[\alpha,\gamma]^g)$. It will then follow from (26) that $Z(P^+[\alpha,\gamma]) \leq qZ(P[\alpha,\gamma])^2$.

Define the channels

$$\begin{aligned} P^+_{u_1v_1}[\alpha,\gamma](y_1,y_2 \mid s) &= q^2 P^+[\alpha,\gamma](y_1,y_2,u_1,u_2 \mid s), \\ P_x[\alpha,\gamma]^g(y_1,y_2 \mid s) &= qP[\alpha,\gamma]^g(y_1,y_2,x \mid s). \end{aligned}$$

An inspection of (28) and (29) reveals that

$$P_x[\alpha,\gamma]^g(y_1,y_2 \mid s) = \sum_{\alpha u_1+\gamma v_1=x} \tfrac{1}{q} P^+_{u_1v_1}[\alpha,\gamma](y_1,y_2 \mid s).$$

Also, we clearly have

$$\begin{aligned} Z(P^+[\alpha,\gamma]) &= \tfrac{1}{q^2}\sum_{u_1,v_1} Z(P^+_{u_1v_1}[\alpha,\gamma]), \\ Z(P[\alpha,\gamma]^g) &= \tfrac{1}{q}\sum_x Z(P_x[\alpha,\gamma]^g). \end{aligned}$$

It then follows from the concavity of the Bhattacharyya parameter in the channel (cf. Lemma 32 below) that

$$\begin{aligned} Z(P[\alpha,\gamma]^g) &= \tfrac{1}{q}\sum_x Z(P_x[\alpha,\gamma]^g) \\ &= \tfrac{1}{q}\sum_x Z\left(\sum_{\alpha u_1+\gamma v_1=x} \tfrac{1}{q} P^+_{u_1v_1}[\alpha,\gamma]\right) \\ &\geq \tfrac{1}{q^2}\sum_x \sum_{\alpha u_1+\gamma v_1=x} Z(P^+_{u_1v_1}[\alpha,\gamma]) \\ &= \tfrac{1}{q^2}\sum_{u_1,v_1} Z(P^+_{u_1v_1}[\alpha,\gamma]) \\ &= Z(P^+[\alpha,\gamma]), \end{aligned}$$

completing the proof.

Lemma 32: Let $Q, Q_1, \ldots, Q_K$ be q-ary input channels with

$$Q = \sum_{k=1}^K p_k Q_k,$$

where $p_k \geq 0$ and $\sum_k p_k = 1$. Then,

$$Z(Q) \geq \sum_{k=1}^K p_k Z(Q_k).$$

Proof: The proof is identical to that of [1, Lemma 4]:

$$\begin{aligned}
Z(Q) &= \frac{1}{q-1}\left[-1+\frac{1}{q}\sum_{y}\left(\sum_{x}\sqrt{Q(y\mid x)}\right)^2\right] \\
&\geq \frac{1}{q-1}\left[-1+\frac{1}{q}\sum_{y}\sum_{k}p_k\left(\sum_{x}\sqrt{Q_k(y\mid x)}\right)^2\right] \\
&= \sum_{k} p_k Z(Q_k).
\end{aligned}$$

Here, the inequality follows from [8, p. 524, ineq. (h)]. ∎

APPENDIX C

Lemma 33: Let $X, W \in \mathbb{F}_q$ be independent and uniformly distributed random variables, and let Y be an arbitrary random variable. For every $\epsilon > 0$, there exists $\delta > 0$ such that

(i) $I(X;Y) < \delta$, $I(W;Y) < \delta$, $H(X \mid YW) < \delta$, $H(W \mid YX) < \delta$ and

(ii) $H(\alpha X + \gamma W \mid Y) \notin (\delta, 1-\delta)$ for all $\alpha, \gamma \in \mathbb{F}_q$,

implies

$$I(\alpha' X + \gamma' W; Y) > 1 - \epsilon.$$

for some $\alpha', \gamma' \in \mathbb{F}_q$.

Proof: Let π be a permutation on $\mathbb{F}_q$, and let

$$p_\pi(x,w) = \begin{cases} \frac{1}{q} & \text{if } w = \pi(x) \\ 0 & \text{otherwise} \end{cases}.$$

Note that $H(X) = H(W) = 1$ and $H(W \mid X) = H(X \mid W) = 0$ whenever (X,W) is distributed as p_π. We claim that for every π, there exist $\alpha_\pi, \gamma_\pi \in \mathbb{F}_q \backslash \{0\}$ such that

$$H(\alpha_\pi X + \gamma_\pi W) < 1 - c(q),$$

where $c(q) > 0$ depends only on q. To see this, given a permutation π, let

$$\alpha_\pi := \pi(0) - \pi(1), \quad \gamma_\pi := 1, \quad \mu := \pi(0). \tag{34}$$

Clearly, $\alpha_\pi \neq 0$. It is also easy to check that with these definitions we have

$$\Pr[\alpha_\pi X + \gamma_\pi W = \mu] \geq \Pr[(X,W) = (0,\pi(0))] + \Pr[(X,W) = (1,\pi(1))] = \tfrac{2}{q},$$

which yields the claim. It also follows from the continuity of entropy in the L_1 metric that

$$\|p_{XW} - p_\pi\| \leq \epsilon \quad \text{implies} \quad H(\alpha_\pi X + \gamma_\pi W) \leq (1 - c(q))(1 - o(\epsilon))^{-1}.$$

We now show that for every $\epsilon > 0$, there exists a $\delta > 0$ such that whenever $H(W|YX) < \delta$, $H(X|YW) < \delta$, $I(W;Y) < \delta$ and $I(X;Y) < \delta$, then there is a set S of y's with $p_Y(S) > 1 - \epsilon$ such that for all $y \in S$

$$\min_\pi \|p_{XW|Y=y} - p_\pi\|_1 < \epsilon.$$

From $I(W;Y) < \delta$, Pinsker's inequality yields

$$\sum_y p_Y(y)\|\tfrac{1}{q} - p_{W|Y=y}\|_1 < \sqrt{2\delta \ln 2} < 2\sqrt{\delta},$$

and we conclude that the set

$$G := \{y : \|\tfrac{1}{q} - p_{W|Y=y}\|_1 < \delta^{1/4}\}$$

has probability at least $1 - 2\delta^{1/4}$. Note that for $y \in G$,

$$\begin{aligned}
\tfrac{1}{q} - \tfrac{1}{q}\delta^{1/4} < p_{W|Y=y}(0|y) < \tfrac{1}{q} + \tfrac{1}{q}\delta^{1/4} \\
\tfrac{1}{q} - \tfrac{1}{q}\delta^{1/4} < p_{W|Y=y}(1|y) < \tfrac{1}{q} + \tfrac{1}{q}\delta^{1/4}
\end{aligned}$$

and thus

$$\begin{aligned}
(1-\delta^{1/4})p_Y(y) < p_{Y|W}(y|0) < (1+\delta^{1/4})p_Y(y) \\
(1-\delta^{1/4})p_Y(y) < p_{Y|W}(y|1) < (1+\delta^{1/4})p_Y(y)
\end{aligned}$$

Furthermore, as

$$\delta > H(X|WY) = \sum_{w,y} p_{WY}(w,y) H(X|W=w, Y=y),$$

the set $\{(w,y)\colon H(X|W=w,Y=y) > \sqrt{\delta}\}$ has probability at most $\sqrt{\delta}$. Let

$$B_w = \{y\colon H(X|W=w,Y=y) > \sqrt{\delta}\}, \quad w \in \mathbb{F}_q \text{ and } B = \cup_w B_w.$$

Then,

$$\begin{aligned} P_Y(G\cap B_w) &= \sum_{y\in G\cap B_w} p_Y(y) \\ &\le [1-\delta^{1/4}]^{-1} \sum_{y\in G\cap B_w} p_{Y|W}(y|w) \\ &\le [1-\delta^{1/4}]^{-1} \sum_{y\in B_w} p_{Y|W}(y|w) \\ &\le [1-\delta^{1/4}]^{-1} 2 \sum_{y\in B_w} p_{WY}(w,y) \\ &\le [1-\delta^{1/4}]^{-1} 2\sqrt{\delta} \end{aligned}$$

for all $w \in \mathbb{F}_q$, and thus

$$P_Y(G\cap B) \le 2q\sqrt{\delta}[1-\delta^{1/4}]^{-1},$$

and the set $S = G\cap B^c$ has probability

$$P_Y(S) > 1 - 2\delta^{1/4} - 2q\sqrt{\delta}/[1-\delta^{1/4}] = 1 - o(\delta).$$

Note that for all $y\in S$ we have for any w, $|\frac{1}{q} - p_{W|Y=y}(w)| < o(\delta)$, and $p_{X|WY}(x|w,y) \notin (o(\delta), 1-o(\delta))$, and thus

$$\min_\pi \|p_{WX|Y=y} - p_\pi\| < o(\delta).$$

In particular, this implies that there exist π' and $S' \subset S$ with $P_Y(S') \ge P_Y(S)/q!$ such that

$$\|p_{WX|Y=y} - p_{\pi'}\| < o(\delta)$$

for all $y \in S'$. Letting $\alpha' = \alpha_{\pi'}$ and $\gamma' = \gamma_{\pi'}$, where $\alpha_{\pi'}$ and $\gamma_{\pi'}$ are defined as in (34), we obtain

$$\begin{aligned} H(\alpha' X + \gamma' W \mid Y) &\le P_Y(S')(1-c(q))(1-o(\epsilon))^{-1} + P_Y(S'^c) \\ &= (1-c_2)(1-o(\epsilon))^{-1} \end{aligned}$$

where $c_2 > 0$ depends only on q. Noting that $I(\alpha' X + \gamma' W; Y) \notin (\delta, 1-\delta)$ by assumption, and that

$$\begin{aligned} I(\alpha' X + \gamma' W; Y) &= H(\alpha' X + \gamma' W) - H(\alpha' X + \gamma' W \mid Y) \\ &\ge 1 - (1-c_2)(1-o(\epsilon))^{-1}, \end{aligned}$$

we see that if δ is sufficiently small, then $I(\alpha' X + \gamma' W; Y) \ge 1-\delta$. ■

REFERENCES

[1] E. Arıkan, “Channel polarization: a method for constructing capacity-achieving codes for symmetric binary input memoryless channels,” *IEEE Trans. Inform. Theory*, vol. 55, pp. 3051–3073, Jul. 2009.

[2] B. Rimoldi, R. Urbanke, “A rate-splitting approach to the gaussian multiple-access channel,” *IEEE Trans. Inform. Theory*, vol. 42, pp. 364–375, Mar. 1996.

[3] A. J. Grant, B. Rimoldi, R. L. Urbanke, P. A. Whiting, “Rate-splitting multiple access for discrete memoryless channels,” *IEEE Trans. Inform. Theory*, vol. 47, pp. 873–890, Mar. 2001.

[4] E. Arıkan, E. Telatar, “On the rate of channel polarization,” *Proc. Int. Symp. Inform. Theory*, pp. 1493–1495, Jul. 2009.

[5] E. Şaşoğlu, E. Telatar, E. Arıkan, “Polarization for arbitrary discrete memoryless channels,” Aug. 2009, [Online]. Available: arXiv0908.0302 [cs.IT].

[6] E. Şaşoğlu, “An entropy inequality for *q*-ary random variables and its application to channel polarization,” *Proc. Int. Symp. Inform. Theory*, Jun. 2010.

[7] E. Abbe, E. Telatar, “MAC polar codes and matroids,” *Proc. Inform. Theory and App. Workshop (ITA),*” 2010.

[8] R. G. Gallager, *Information Theory and Reliable Communication.* New York: Wiley, 1968.